pulverization, burning, melting, incineration, shredding or sanding, are acceptable.

(2) Disposal methods are considered adequate if the personal data is rendered unrecognizable or beyond reconstruction.

§ 310.14 Notification when information is lost, stolen, or compromised.

(a) If records containing personal information are lost, stolen, or compromised, the potential exists that the records may be used for unlawful purposes, such as identity theft, fraud, stalking, etc. The personal impact on the affected individual may be severe if the records are misused. To assist the individual, the Component shall promptly notify the individual of any loss, theft, or compromise (See also, § 310.50 for reporting of the breach to Senior Component Official for Privacy and the Defense Privacy Office).

(1) The notification shall be made whenever a breach occurs that involves personal information pertaining to a service member, civilian employee (appropriated or non-appropriated fund), military retiree, family member, DoD contractor, other persons that are affiliated with the Component (e.g., volunteer), and/or any other member of the public on whom information is maintained by the Component or by a contractor on behalf of the Component.

(2) The notification shall be made as soon as possible, but not later than 10 working days after the loss, theft, or compromise is discovered and the identities of the individuals ascertained.

(i) The 10 day period begins to run after the Component is able to determine the identities of the individuals whose records were lost.

(ii) If the Component is only able to identify some but not all of the affected individuals, notification shall be given to those that can be identified with follow-up notifications made to those subsequently identified.

(iii) If the Component cannot readily identify the affected individuals or will not be able to identify the individuals, the Component shall provide a generalized notice to the potentially impacted population by whatever means the Component believes is most likely to reach the affected individuals.

(3) When personal information is maintained by a DoD contractor on behalf of the Component, the contractor shall notify the Component immediately upon discovery that a loss, theft or compromise has occurred.

(i) The Component shall determine whether the Component or the contractor shall make the required notification.

(ii) If the contractor is to notify the impacted population, it shall submit the notification letters to the Component for review and approval. The Component shall coordinate with the Contractor to ensure the letters meet the requirements of § 310.14.

(4) Subject to paragraph (a)(2) of this section, the Component shall inform the Deputy Secretary of Defense of the reasons why notice was not provided to the individuals or the affected population within the 10-day period.

(i) If for good cause (e.g., law enforcement authorities request delayed notification as immediate notification will jeopardize investigative efforts), notice can be delayed, but the delay shall only be for a reasonable period of time. In determining what constitutes a reasonable period of delay, the potential harm to the individual must be weighed against the necessity for delayed notification.

(ii) The required notification shall be prepared and forwarded to the Senior Component Official for Privacy who shall forward it to the Defense Privacy Office. The Defense Privacy Office, in coordination with the Office of the Under Secretary of Defense for Personnel and Readiness, shall forward the notice to the Deputy Secretary.

(5) The notice to the individual, at a minimum, shall include the following:

(i) The individuals shall be advised of what specific data was involved. It is insufficient to simply state that personal information has been lost. Where names, social security numbers, and dates of birth are involved, it is critical that the individual be advised that these data elements potentially have been compromised.

(ii) The individual shall be informed of the facts and circumstances surrounding the loss, theft, or compromise. The description of the loss should be sufficiently detailed so that

the individual clearly understands how the compromise occurred.

(iii) The individual shall be informed of what protective actions the Component is taking or the individual can take to mitigate against potential future harm. The Component should refer the individual to the Federal Trade Commission's public Web site on identity theft at *http://www.consumer.gov/idtheft/con_steps.htm*. The site provides valuable information as to what steps individuals can take to protect themselves if their identities potentially have been or are stolen.

(iv) A sample notification letter is at appendix B.

(b) The notification shall be made whether or not the personal information is contained in a system of records (See §310.10(a)).

Subpart C—Collecting Personal Information

§310.15 General considerations.

(a) *Collect directly from the individual.* Collect to the greatest extent practicable personal information directly from the individual to whom it pertains if the information may result in adverse determination about an individual's rights, privileges, or benefits under any Federal program.

(b) *Collecting social security numbers (SSNs).* (1) It is unlawful for any Federal, State, or local governmental agency to deny an individual any right, benefit, or privilege provided by law because the individual refuses to provide his or her SSN. However, if a Federal statute requires the SSN be furnished or if the SSN is furnished to a DoD Component maintaining a system of records in existence that was established and in operation before January 1, 1975, and the SSN was required under a statute or regulation adopted prior to this date for purposes of verifying the identity of an individual, this restriction does not apply.

(2) When an individual is requested to provide his or her SSN, he or she must be told:

(i) What uses will be made of the SSN;

(ii) The statute, regulation, or rule authorizing the solicitation of the SSN; and

(iii) Whether providing the SSN is voluntary or mandatory.

(3) Include in any systems notice for any system of records that contains SSNs a statement indicating the authority for maintaining the SSN.

(4) E.O. 9397,"Numbering System for Federal Accounts Relating to Individual Persons", November 30, 1943, authorizes solicitation and use of SSNs as a numerical identifier for Federal personnel that are identified in most Federal record systems. However, it does not constitute authority for mandatory disclosure of the SSN.

(5) Upon entrance into military service or civilian employment with the Department of Defense, individuals are asked to provide their SSNs. The SSN becomes the service or employment number for the individual and is used to establish personnel, financial, medical, and other official records. The notification in paragraph (b)(2) of this section shall be provided the individual when originally soliciting his or her SSN. The notification is not required if an individual is requested to furnish his SSN for identification purposes and the SSN is solely used to verify the SSN that is contained in the records. However, if the SSN is solicited and retained for any purposes other than verifying the existing SSN in the records, the requesting official shall provide the individual the notification required by paragraph (b)(2) of this section.

(6) Components shall ensure that the SSN is only collected when there is a demonstrated need for collection. If collection is not essential for the purposes for which the record or records are being maintained, it should not be solicited.

(7) DoD Components shall continually review their use of the SSN to determine whether such use can be eliminated, restricted, or concealed in Component business processes, systems and paper and electronic forms. While use of the SSN may be essential for program integrity and national security when information about an individual is disclosed outside the DoD, it may not be as critical when the information is being used for internal Departmental purposes.